RECEIVED
CENTRAL FAX CENTER
JUN 2 2 2007

SPECIFICATION AMENDMENTS

Please replace paragraph [0003] with the following rewritten paragraph:

[0003] Security is an issue in this kind of network as the communication media used is shared. As a result, wireless networks are particularly vulnerable to attacks at the lowest levels of the communication protocols (first and second layer of the Open Systems Interconnection (OSI) model). It is indeed very easy to tap or inject traffic into such a network.

Please replace paragraph [0005] with the following rewritten paragraph:

[0005] Traditional security systems and technologies such are firewall or IP Security (IPSec) tunnel fail to fully address those threats since they are not designed to address security threats at lower levels of the OSI model. Other mechanisms, such as address filtering performed by the wireless equipment, are useless in this environment where impersonating a valid address is so easy to do.

Please replace paragraph [0009] with the following rewritten paragraph:

[0009] These security services are especially important for wireless communication, due to the ease of tapping into wireless networks. In addition, since firewalls are employed on the user side of a wireless link, a message rejected by the firewall has already consumed the wireless resources required to transmit. The wireless links are supported by Radio Frequency (RF) channels, which are a scarce resource. Accordingly, messages rejected by the firewall tend to waste bandwidth which could be allocated to other connections, can drive up user cost by

increasing message transmissions, and tend to slow overall throughput because of the resources required to transmit them over the wireless link.

Please replace paragraph [0010] with the following rewritten paragraph:

[0010] A specificity of wireless networks is that they require IDS-like systems specific to the lower Media Access Control (MAC) layer management element (as defined by the seven-layer OSI model) while traditional IDS systems mainly focus on the third and higher layers of the OSI model.

Plese replace paragraph [0013] with the following rewritten paragraph:

[0013] Joshua Wight, ~~deseribes~~ in an article entitled "Detecting Wireless LAN MAC Address Spoofing", ~~publication date not provided, available at http://www.polarcove.com/whitepapars/detectwireless.pdf,~~ provides an in-depth analysis of the anomalies generated by tools that spoof MAC addresses. While knowledge of these anomalies enables an easier detection of the spoofed traffic generated by these tools, the analysis has some limitations. For example, it is based on anomalies generated by specific attack tools, which should not be considered as invariants. As well, most of the anomalies are present when random MAC addresses are used for attacks, which is not always the case.